GNFS による因数分解例(3 次多項式)

2006/02/12　後　保範
2006/11/13　指摘訂正

1. 合成数に対応する関数

$N=1333$ を GNFS で因数分解する。

$f(x)=x^3+2,\quad M=11,\quad f(M)=N$

2. 素数と素イデアルの作成

p を素数とし、 $f(x)=(x-s)g(x) \bmod p$ となる p と s の組を求める。

これは、 $f(s)=0 \bmod p$ より (p,s) の組を求めることに対応する。

下記に $p=31$ までの素数に対応する素イデアル (p,s) の組を示す。

p	2	3	5	7	11	13	17	19	23	29	31
s	0	1	2	---	4	---	-8	---	7	3	-4
	---	---	---	---	---	---	---	---	---	---	-7
	---	---	---	---	---	---	---	---	---	---	11

3. 素数及び素イデアルによる因数分解

(1) 使用する素数と素イデアル

素数 p は 2～19 まで使用し P1～P8 に対応させる。

即ち、P1=2, P2=3, P3=5, P4=7, P5=11, P6=13, P7=17, P8=19 とする。

素イデアルは分解用(Q)と平方剰余用(R)の 2 種類に分ける。

分解用イデアル Q(p;s)として Q1(2;0), Q2(3;1), Q3(5;2), Q4(11;4), Q5(17;-8), Q6(23;7)を使用する。

平方剰余用イデアル R(p;s)として R1(29;3), R2(31;-7)を使用する。

(2) 素数での分解

$a+bM$ を素数 P1～P8 で完全に分解されたものを選ぶ。

(3) 素イデアルによる分解

イデアル $a+b\theta$ に対すノルムを $N(a,b)=\left|b^3 f\left(-\frac{a}{b}\right)\right|=\left|a^3-2b^3\right|$ で与える。

$N(a,b)$ がイデアル $a+b\theta$ を素イデアル $Q_k(p_k;s_k)$ で分解するには、 $N(a,b)$ を p_k で完全に分解されるものを選ぶ。

$N(a,b)$ が p_k で割れることと、$a+bs_k$ が p_k で割れることは同じであり、高速化のため、まず $a+bs_k$ が p_k で割れる p_k を選び、その p_k で $N(a,b)$ が完全に分解されるかのテストを行う。

(4) 素イデアルによる平方剰余の計算

素数と素イデアルにより共に分解されたイデアル$a+b\theta$に対して各 R(p;s)で平方剰余になるか非平方剰余になるか調べ、平方剰余なら 0 を非平方剰余なら 1 とする。平方剰余のテストは$a-bs$が p の平方剰余かどうか、即ち$(a-bs)^{(p-1)/2} \bmod p$を計算し、その結果が 1 なら 0 を-1 なら 1 とする。$a-bs$が p の倍数なら平方剰余で 0 とする。

注）通常は$a+bs$の平方剰余を使用している。$a-bs$でも確率的に同じ。

(5) 分解結果

No	a	b	P1	P2	P3	P4	P5	P6	P7	P8	Q1	Q2	Q3	Q4	Q5	Q6	R1	R2
1	-7	1	2	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
2	-4	1	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	1
3	-2	1	0	2	0	0	0	0	0	0	1	0	1	0	0	0	0	0
4	-1	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
5	1	1	2	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
6	2	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0
7	3	1	1	0	0	1	0	0	0	0	0	0	2	0	0	0	0	0
8	8	1	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1
9	-1	2	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1
10	3	2	0	0	2	0	0	0	0	0	0	0	0	1	0	0	1	1
11	-1	3	5	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
12	2	3	0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	1
13	7	3	3	0	1	0	0	0	0	0	0	0	0	0	2	0	1	0
14	-5	4	0	1	0	0	0	1	0	0	0	0	0	1	0	1	1	1
15	5	4	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	0
16	2	5	0	1	0	0	0	0	0	1	1	0	0	2	0	0	0	1

4. 従属行の計算

(1) 行列の作成（A、Eのサイズは共に 16×16）

(a) 分解結果の P,Q,R の部分の値に対して 2 の剰余にした行列を作成する。
この行列をAとするとAは n×m の行列になる。

(b) 上記行列の右に単位行列を追加する。
この行列をEとするとEは n×n の単位行列になる。

(2) 行列の消去計算

(a) (A+E)行列のA部分において行交換を伴う消去計算(2 の剰余)を行う。

(b) 消去対応列が全てゼロの時は消去列を右にずらす。

(3) 従属行の取り出し

(a) 行列Aの消去完了したとき、消去された行列Eに従属行が得られる。

(b) 行列Aの行全体がゼロになる行番号に対応する行列Eの中の 1 となる列番号を取り出すと、従属行の番号が得られる。

(4) 具体的計算

(a) 作成した行列

N0.	行列A	行列E
1	0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
2	0 0 0 1 0 0 0 0 1 1 0 1 0 0 0 1	0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
3	0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0	0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
4	1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1	0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
5	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0	0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
6	0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0	0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
7	1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
8	0 0 0 0 0 0 0 1 1 1 1 0 1 0 0 1	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
9	0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 1	0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
10	0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 1	0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0
11	1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 0	0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0
12	0 0 1 1 0 0 0 0 1 0 0 0 0 1 0 1	0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0
13	1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0	0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0
14	0 1 0 0 0 1 0 0 0 0 0 1 0 1 1 1	0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
15	0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0
16	0 1 0 0 0 0 0 1 1 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0

(b) 消去した行列

No.	行列A	行列E
1	1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1	0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
2	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0	0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
3	0 0 1 1 0 0 0 0 0 1 0 0 0 0 0 1	0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0
4	0 0 0 1 0 0 0 0 1 1 0 1 0 0 0 1	0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
5	0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0	0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
6	0 0 0 0 0 0 0 1 1 1 1 0 1 0 0 1	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
7	0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0	0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
8	0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
9	0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1	1 1 1 0 0 0 1 0 0 0 1 0 0 0 0 0
10	0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 1	0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0
11	0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1	1 1 1 0 1 0 0 0 1 1 0 0 0 0 0 0
12	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0	1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0
13	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	1 1 0 1 0 0 0 0 0 0 1 1 0 0 1 0
14	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 1 0 1 1 0 0 0 1 0 0 0 1 0 0
15	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 1 1 0 0 1 0 0 0 1 0 1 0 0 0
16	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 1 1

(c) 取り出した従属行

No. 14 : 1, 3, 5, 6, 10, 14

No. 15 : 2, 3, 4, 7, 11, 13

No. 16 : 7, 8, 9, 10, 11, 15, 16

5. イデアルの平方根の計算

(1) 素数の平方根とイデアルの平方根の関係

従属関係が成り立つように選定した行をkとし、分解する素数P_jのベキをL_jとすると、L_jは偶数で下記の関係が成立する。

$$\prod_j (a_j + b_j M) = \left(\prod_j P_j^{L_j/2} \right)^2 = P^2 \mod N$$

また、イデアルの方も従属関係が成立しているので、下記の関係が成立する確率が高い。平方剰余Rを追加したのはこの$F(\theta)$と$B(\theta)$の平方関係の確率を高めるためである。

$$\prod_j (a_j + b_j \theta) = F(\theta) = B(\theta)^2 \mod f(\theta)$$

もし、上式が成立するなら$f(M) = N$のため下記が成立する。

$$P^2 = B(M)^2 \mod N$$

(2) イデアルの平方根の関係式

$f(x) = x^3 + Ax^2 + Bx + C, \quad f(M) = N$とする。

今回の例では、$A = B = 0, C = 2, M = 11, N = 1333$である。

$F(\theta) = a\theta^2 + b\theta + c, \quad B(\theta) = x_1\theta^2 + x_2\theta + x_3$とすると$F(\theta) = B(\theta)^2 \mod f(\theta)$から次の$x_1, x_2, x_3$を未知数とする非線形連立方程式が得られる。

$$g_1(x) = (A^2 - B)x_1^2 - 2Ax_1x_2 + x_2^2 + 2x_1x_3 - a = 0$$
$$g_2(x) = (AB - C)x_1^2 - 2Bx_1x_2 + 2x_2x_3 - b = 0$$
$$g_3(x) = ACx_1^2 - 2Cx_1x_2 + x_3^2 - c = 0$$

上記方程式の数値解x_1, x_2, x_3の中で、x_1, x_2, x_3全てが整数となるものが求めるものである。これにより整数係数の関数$B(\theta)$が求まる。

今回の場合は$A = B = 0, C = 2$のため下記の方程式となる。

$$g_1(x) = x_2^2 + 2x_1x_2 - a = 0$$
$$g_2(x) = -2x_1^2 + 2x_2x_3 - b = 0$$
$$g_3(x) = -4x_1x_2 + x_3^2 - c = 0$$

整数解が求まらない場合は$F(\theta) = B(\theta)^2 \mod f(\theta)$の関係が成立しないためであり、別のイデアルの平方根を求める。

(3) 非線形方程式の計算

擬似ニュートン法を使用して下記の式を反復計算して求める。

$$J(x^{(k)})\Delta x = g(x^{(k)})$$
$$x^{(k+1)} = x^{(k)} - \Delta x$$

ここで、$x = (x_1, x_2, x_3)^T, g = (g_1, g_2, g_3)$で$J$は下記のヤコービアンである。

$$J(x)=\begin{pmatrix} \partial g_1/\partial x_1 & \partial g_1/\partial x_2 & \partial g_1/\partial x_3 \\ \partial g_2/\partial x_1 & \partial g_2/\partial x_2 & \partial g_2/\partial x_3 \\ \partial g_3/\partial x_1 & \partial g_3/\partial x_2 & \partial g_3/\partial x_3 \end{pmatrix}$$

$$=2\begin{pmatrix} (A^2-B)x_1-Ax_2+x_3 & -Ax_1+x_2 & x_1 \\ (AB-C)x_1-Bx_2 & -Bx_1+x_3 & x_2 \\ C(Ax_1-x_2) & -Cx_1 & x_3 \end{pmatrix}$$

今回の例では $A=B=0,\ C=2$ のため $J(x)$ は下記のようになる。

$$J(x)=2\begin{pmatrix} x_3 & x_2 & x_1 \\ -2x_1 & x_3 & x_2 \\ -2x_2 & -2x_1 & x_3 \end{pmatrix}$$

(4) 具体的計算

(a) No. 14

(1, 3, 5, 6, 10, 14)行に対応するイデアルの乗算から下記が得られる。

$$F(\theta)=(\theta-7)(\theta-2)(\theta+1)(\theta+2)(2\theta+3)(4\theta-5)$$
$$=529\theta^2-74\theta-908 \mod f(\theta)$$

これより下記の連立方程式が成立する。

$$g_1(x)=x_2^2+2x_1x_2-529=0$$
$$g_2(x)=-2x_1^2+2x_2x_3+74=0$$
$$g_3(x)=-4x_1x_2+x_3^2+908=0$$

この方程式の整数解は $x_1=11, x_2=21,\ x_3=4$ となり、下記が成立する。

$$F(\theta)^{1/2}=B(\theta)=11\theta^2+21\theta+4 \mod f(\theta)$$
$$B(11)=233 \mod 1333$$

(b) No. 15

(2, 3, 4, 7, 11, 13)行に対応するイデアルの乗算から下記が得られる。

$$F(\theta)=(\theta-4)(\theta-2)(\theta-1)(\theta+3)(3\theta-1)(3\theta+7)$$
$$=481\theta^2-386\theta-212 \mod f(\theta)$$
$$F(\theta)^{1/2}=B(\theta)=3\theta^2+23\theta-8 \mod f(\theta)$$
$$B(11)=608 \mod 1333$$

(c) No. 16

(7, 8, 9, 10, 11, 15, 16)行に対応するイデアルの乗算から下記が得られる。

$$F(\theta)=(\theta+3)(\theta+8)(2\theta-1)(2\theta+3)(3\theta-1)(4\theta+5)(5\theta+2)$$
$$=-31247\theta^2-28292\theta+13972 \mod f(\theta)$$

$$F(\theta)^{1/2} = B(\theta) = 108\theta^2 + 17\theta + 146 \mod f(\theta)$$
$$B(11) = 1112 \mod 1333$$

6. 素数の平方根と因数分解

(1) 平方根計算のための各素数のべき乗

具体的計算を参照。

(2) 素数の平方根の計算

具体的計算を参照。

(3) 因数分解

具体的計算を参照。

3 件総てでイデアルの平方根が求まった。

通常、因数分解できる解と自明解が半分の確率で発生するが、今回は 3 件総てで因数分解できる。

(4) 具体的計算

(a) No. 14

(1, 3, 5, 6, 10, 14)行を合計した P1～P8 のベキは(4, 4, 2, 0, 0, 2, 0, 0)となる。

従って求める素数の積の平方根 P は下記の様になる。

$$P = P_1^2 P_2^2 P_3^1 P_6^1 \mod N = 2^2 \cdot 3^2 \cdot 5 \cdot 13 \mod 1333 = 1007$$

これより、イデアルの平方根との関係式は

$$1007^2 = B(11)^2 = 233^2 \mod 1333$$

となる。従って、因数分解結果は下記のようになる。

$$GCD(1007 + 233, 1333) = 31$$
$$GCD(1007 - 233, 1333) = 43$$

(b) No. 15

(2, 3, 4, 7, 11, 13)行を合計した P1～P8 のベキは(10, 2, 2, 2, 0, 0, 0, 0)となる。

従って求める素数の積の平方根 P は下記の様になる。

$$P = P_1^5 P_2^1 P_3^1 P_4^1 \mod N = 2^5 \cdot 3^1 \cdot 5 \cdot 7 \mod 1333 = 694$$

これより、イデアルの平方根との関係式は

$$694^2 = B(11)^2 = 608^2 \mod 1333$$

となる。従って、因数分解結果は下記のようになる。

$$GCD(694 + 608, 1333) = 31$$
$$GCD(694 - 608, 1333) = 43$$

(c) No. 16

(7, 8, 9, 10, 11, 15, 16)行を合計した P1～P8 のベキは(6, 2, 2, 4, 0, 0, 0, 2)となる。

従って求める素数の積の平方根 P は下記の様になる。

$$P = P_1^3 P_2^1 P_3^1 P_4^2 P_8^1 \mod N = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^2 \cdot 19^1 \mod 1333 = 1081$$

これより、イデアルの平方根との関係式は

$$1081^2 = B(11)^2 = 1112^2 \mod 1333$$

となる。従って、因数分解結果は下記のようになる。

$$GCD(1112 + 1081, 1333) = 43$$

$$GCD(1112 - 1081, 1333) = 31$$